INTRUSION DETECTION

James M. Doherty
Thomas Lee Adams
Steve Mueller

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a continuation-in-part of "HOST INTRUSION DETECTION AND ISOLATION", U.S. Patent Application Serial No. 10/634,117, filed August 24, 2003, having Attorney Docket No. T00534, pending, whose contents are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

Field of Invention

[0002] The present invention relates generally to the field of computer and network security. More specifically, the present invention is related to intrusion detection and isolation.

Discussion of Prior Art

[0003] Prior art solutions proposed to prevent intrusion in a host system fall under two main categories: external protection or internal protection. External protection scenarios include (but are not limited to) firewalls and routers which provide protection against various attacks (e.g., denial of service or DoS attacks) on a network infrastructure. The firewall approach prevents unauthorized access from an outsider (such as, an unauthorized user or hacker) by monitoring traffic on critical incoming ports. The firewall security layer is a control layer inserted between a local private network and an outside internet network. The firewall security layer permits only some traffic to pass through. The firewall is configured by a host master of the local private network based on the local private network's security policy. For example, the firewall can be configured to block: (a) traffic of a certain type, (b) traffic from certain addresses, or (c)

traffic from all but a predetermined set of IP addresses. Firewalls also provide several schemes such as port forwarding and DMZ type applications. Additionally, they can, but often do not, limit outgoing port connections. The firewall, moreover, cannot block all IP addresses. An attacker (outsider, unauthorized user or hacker) is able to exploit this vulnerability. In this scenario, the attacker masks any harmful intent at the beginning of a session, gains access to sensitive data, and at a later point, attacks the host system. The firewall security layer has to update the harmful addresses after such attack or intrusion occurred. Thus, the firewall solution fails to offer a real-time blocking solution with regard to such harmful IP addresses.

[0004] Internal protection schemes have been designed to prevent breaches in security through the use of file permission, directory access, and execution permission usually set as part of the file system associated with the host. This prevents unauthorized users from accessing sensitive aspects of the system.

[0005] The question of how to determine, programmatically, that a system has been breached is a interesting problem. There have been several efforts in the industry that only partial solutions to address this issue.

[0006] Whatever the precise merits, features, and advantages of the above mentioned prior art internal or external protection schemes, none of them achieves or fulfills the purposes of the present invention.

SUMMARY OF THE INVENTION

[0007] The present invention provides for a method to detect intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities (e.g., system files, configuration files, directories, etc) to be monitored. The method as implemented in the host comprises the steps of: (a) monitoring data entities via comparing a locally stored copy of a digital signature (e.g., an MD5 signature) associated with each data entity against a corresponding digital signature stored in a first remote database (e.g., an MD5 database); and (b) upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database (e.g., a SYSLOG database), said entry identifying a possible intrusion in said host. In one embodiment, the host communicates with the first (e.g., an MD5 database) and second (e.g., a SYSLOG database) remote databases via one or more network interfaces and, subsequent to the above-mentioned step (b), the method further comprises the step of issuing a command to bring down the network interfaces to isolate the host. In another embodiment, the method comprises the additional step of issuing a command to the operating system of the host to bring it to a single user state.

[0008] In an extended embodiment, the first remote database (e.g., an MD5 database) and the second remote database (e.g., a SYSLOG database) are located on a single server or, alternatively, on a plurality of servers belonging to a common local area network.

[0009] In another embodiment, communications between the host and first remote database (e.g., an MD5 database) and communications between the host and second remote database (e.g., an SYSLOG database) are encrypted (for example, via the secure shell protocol).

[0010] The present invention also provides for a system to detect intrusion comprising: (a) a host running a monitoring daemon working in conjunction with a configuration file (the configuration file identifies files and directories to be monitored in the host), wherein the host communicates with external networks via one or more network interfaces and the

monitoring daemon dynamically monitors the files and directories identified by the configuration file by comparing a locally stored digital signature corresponding to each file or directory against a remotely stored corresponding digital signature; (b) a digital signature database located remotely from the host and storing the digital signatures associated with files and directories identified by the configuration file; and (c) a log database located remotely from the host and recording entries corresponding to mismatches between a digital signature stored in said host and a corresponding digital signature in the digital signature database.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG.1 illustrates an exemplary embodiment associated with the system of the present invention.

[0012] FIG. 2 illustrates a flow chart outlining one embodiment of the present invention's method for detecting an intrusion in a host system.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0013] While this invention is illustrated and described in a preferred embodiment, the invention may be produced in many different configurations. There is depicted in the drawings, and will herein be described in detail, a preferred embodiment of the invention, with the understanding that the present disclosure is to be considered as an exemplification of the principles of the invention and the associated functional specifications for its construction and is not intended to limit the invention to the embodiment illustrated. Those skilled in the art will envision many other possible variations within the scope of the present invention.

[0014] Figure 1 illustrates an exemplary embodiment associated with the system of the present invention. System daemon (designated as "jtrip" in figure 1) **101** is a daemon that is started through normal system startup procedures. It should be noted that the common UNIX® system is used as an example to illustrate the functionality of the present invention, but other systems can also be used in conjunction with the present invention. Hence, the type of operating system should not be used to limit the scope of the present invention. At start up, system daemon **101** reads (in real-time continuous manner) a configuration file (illustrated as "Jtrip.conf" in figure 1) **104** and determines which directories, normal system files, and configuration files of file system **102** are to be monitored in a real-time continuous manner. An example of a configuration file is provided below (it should be noted that lines marked with a "#" symbol in the configuration file correspond to comments and, hence, the system daemon **101** ignores such statements).

```
#-------------------------------------------------------
# Jtrip Configuration File for intrusion detection daemon
#-------------------------------------------------------
# Directives for script are as follows
# DIR=/bin This tells jtrip to use all members of /bin
# to include in the database
# FILE=/bin/rm This tells jtrip to use only this file
# when creating the database
# CONF=/etc/host this tells jtrip that this is a config
# file and may be checked on a different
# Schedule from other directives this is
# used to check vendor supplied control
# files
#-------------------------------------------------------
DIR=/bin
DIR=/sbin
DIR=/usr/sbin
DIR=/usr/local/sbin
FILE=/etc/hosts.equiv
CONF=/etc/pam.conf
----------------------------------------
```

[0015] The Jtrip.conf configuration file **104** tells Jtrip system daemon **101** which data entities (e.g., directories, files, etc.) of file system **102** are to be monitored in a real-time continuous manner. The data includes a valid digital signature such as a MD5 signature, correct permissions, ownership of the file, and information indicating if the file still exists. An MD5 signature is a cryptographic hash code in a MD5 database **103**. The MD5 signature (a cryptographic hash code) is generated for each receiving file and compared to a previous signature for that file stored in the MD5 database **103**. The system daemon **101** identifies any mismatch between a locally stored digital signature against the remotely stored (at the MD5 database **103**) digital signature. The Jtrip **101** reads valid known MD5 signatures and permissions associated with data entities from the remote MD5 database **103**. If any modification are detected based upon the comparison of the digital signatures, the Jtrip system daemon **101** alarms a root user that an intrusion has taken place. Hence, the Jtrip system daemon **101** can be used to monitor one or more files and/or one or more directories. It should be emphasized that the MD5 database **103** is located at a remote location, whereby it is isolated physically as well as

programmatically from the monitored host system. A SYSLOGD database **106** is also provided at a remote location. It should be emphasized that, just as the MD5 database, the SYSLOGD database **106** is also located at a remote location, whereby it is isolated physically as well as programmatically from the monitored host system.

[0016] In one embodiment, the SYSLOGD database **106** is remote from both the MD5 database **103** and the host system. In an alternate embodiment, the SYSLOGD database and the MD5 database are located on a single server or a plurality of servers belonging to a common network (e.g., local area network).

[0017] Once an intrusion (from outsider, un-authorized user, or hacker) is detected (in real-time continuous manner), any of, or a combination of, the following steps are taken to protect the rest of the host system from the compromised system:

1. a log is written to the remote SYSLOGD database **106** indicating the occurrence of a possible intrusion;

2. an IFCONFIG down command is issued (from Jtrip **101**) to one or more network interface **105** wherein the IFCONFIG down commands isolate the host system from the outside network; and

3. an INIT 1 command is issued (by the Jtrip **101**) to the operating system for taking the host system down to single user state, whereby the INIT 1 command limits the access to a single user and the access is physical to the interface **105**.

[0018] Figure 2 illustrates a flow chart outlining one embodiment of the present invention's method for detecting an intrusion in a host system, wherein the host communicates with external networks via has one or more network interfaces. The method comprising the steps of: (a) reading a configuration file to identify data entities to be monitored on a host – step **202**; (b) for each data entity to be monitored, extracting a digital signature from said host – step **204**; (c) for each data entity to be monitored, querying a remote digital signature database via a network interface and requesting a

digital signature corresponding to the digital signature extracted from the host – step **206**; (d) for each data entity to be monitored, receiving the corresponding digital signature from the remote digital signature database – step **208**; (e) matching digital signature received from said remote digital signature database with digital signature extracted at said host– step **210**; (f) upon identifying a mismatch, transmitting an instruction to a remote log database via the network interface, wherein the instruction is executed in the remote log database to record an entry in a log file indicating a possible intrusion in the host – step **212**; and (g) performing any one of, or a combination of, the following steps:

(i) issuing a command to bring down the network interfaces to isolate the host – step **214**; or

(ii) issuing a command to an operating system of host to bring the host to a single user state – step **216**.

[0019] In another embodiment, communications between the host and SYSLOGD database and communications between the host and the MD5 database are encrypted (for example, via the secure shell protocol).

[0020] Furthermore, the present invention includes a computer program code based product, which is a storage medium having program code stored therein which can be used to instruct a computer to perform any of the methods associated with the present invention. The computer storage medium includes any of, but not limited to, the following: CD-ROM, DVD, magnetic tape, optical disc, hard drive, floppy disk, ferroelectric memory, flash memory, ferromagnetic memory, optical storage, charge coupled devices, magnetic or optical cards, smart cards, EEPROM, EPROM, RAM, ROM, DRAM, SRAM, SDRAM, and/or any other appropriate static or dynamic memory or data storage devices.

[0021] Implemented in computer program code based products are software modules for: (a) monitoring data entities via comparing a locally stored copy of a digital signature (e.g., an MD5 signature) associated with each data entity against a corresponding digital

signature stored in a first remote database (e.g., an MD5 database); (b) upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database (e.g., a SYSLOG database), said entry identifying a possible intrusion in said host; (c) issuing a command to bring down one or more network interfaces to isolate the host; and (d) issuing a command to the operating system of the host to bring it to a single user state.

CONCLUSION

[0022] A system and method has been shown in the above embodiments for the effective implementation of a system and method implementing host intrusion detection and isolation. While various preferred embodiments have been shown and described, it will be understood that there is no intent to limit the invention by such disclosure, but rather, it is intended to cover all modifications and alternate constructions falling within the spirit and scope of the invention, as defined in the appended claims. For example, the present invention should not be limited by host operating system, particular database, type of encryption link between the host and the MD5 database, type of encryption link between the host and the SYSLOGD server, or specific hardware interface.

[0023] The above enhancements are implemented in various computing environments. For example, the present invention may be implemented on a conventional IBM PC or equivalent, multi-nodal system (e.g., LAN, WAN) or networking system (e.g., Internet, WWW, wireless web). All programming related thereto are stored in computer memory, static or dynamic, and may be retrieved by the user in any of: conventional computer storage, display (i.e., CRT) and/or hardcopy (i.e., printed) formats. The programming of the present invention may be implemented by one of skill in the art of network programming.

[0024] The above disclosed subject matter is to be considered illustrative, and not restrictive, and the appended claims are intended to cover all such modifications, enhancements, and other embodiments which fall within the true spirit and scope of the present invention. Thus, to the maximum extent allowed by law, the scope of the present

invention is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.